In the claims:

The following listing of claims will replace all prior listings and versions of the claims.

1. (Original) A method of providing a key container by a key container directory, the key container to be used to secure a message that will be sent from a sender to a recipient, the method comprising the steps of:

receiving a request for the key container from a requestor; and

in response to the request, providing a key container to the requestor that contains a cryptographic key of a gateway that the message will transit and an address of the sender or the recipient.

2. (Original) A method of providing a key container according to claim 1, wherein the key container directory is remote from the gateway, such as external to the network domain of the gateway.

3. (Previously presented) A method of providing a key container according to claim 1, wherein the key container directory is external to the network domain of the recipient.

4. (Previously presented) A method of providing a key container according to claim 1, wherein the message is transmitted from the sender over an insecure computer network, such as the Internet.

5. (Previously presented) A method of providing a key container according to claim 1,wherein the network domain of the recipient is secure.

6. (Previously presented) A method of providing a key container claim 1, wherein the step of providing a key container comprises providing a key container for each gateway that the message will transit.

7. (Previously presented) A method of providing a key container according to claim 1, wherein the method further comprises the step of determining the identity of one or more gateways that the message will transit.

8. (Previously presented) A method of providing a key container according to claim 1, wherein the key container directory provides multiple key containers in the response to the request.

9. (Previously presented) A method of providing a key container according to claim 1, wherein the requestor is the sender of the message and the request includes the address of the recipient.

10. (Original) A method of providing a key container according to claim 9, wherein the step of requesting the key container includes an indication that an encryption key container is requested.

11. (Original) A method of providing a key container according to claim 9, wherein the method further comprises the step of determining what type of key container should be provided to the requestor.

12. (Original) A method of providing a key container according to claims 11, wherein the step of determining comprises determining whether the requestor is the sender of the message, and if so, providing an encryption key container to the requestor.

13. (Previously presented) A method of providing a key container according to claim 11, wherein the step of determining further comprises determining whether the requestor is from the same domain as the gateway, and if not, providing the encryption key container containing the cryptographic key of the recipient's gateway.

14. (Previously presented) A method of providing a key container according to claim 11, wherein the step of determining further comprises determining whether the requestor is from the same domain as the gateway, and if so, providing the encryption key container having the cryptographic key of the requestor's gateway.

15. (Previously presented) A method of providing a key container according to claim 1, wherein the requestor is the gateway and the request includes the address of the sender.

16. (Previously presented) A method of providing a key container according to claim 1, wherein the step of requesting the key container includes an indication that a signing key container is requested.

17. (Previously presented) A method of providing a key container according to claim 1, wherein the method further comprises the step of determining what type of key container should be provided to the requestor.

18. (Previously presented) A method of providing a key container according to claim 17, wherein the step of determining further comprises determining whether the requestor is the gateway, and if so, providing the signing key container containing the cryptographic key of the gateway and the message sender's address.

19. (Previously presented) A method of providing a key container according to claim 18, wherein the sender's address is from the same domain as the gateway.

20. (Previously presented) A method of providing a key container according to claim 11, wherein the step of determining is based on parameters associated with the request.

21. (Previously presented) A method of providing a key container according to claim 1, wherein the method further comprises the step of the requestor authenticating with the key container directory.

22. (Previously presented) A method of providing a key container according to claim 21, wherein the method further comprises the step of the requestor authenticating with the key container directory and the step of determining is based on the information provided by the requestor when authenticating with the key container directory.

23. (Previously presented) A method of providing a key container according to claim 21, wherein the step of authenticating is through the use of a valid username and password combination.

24. (Previously presented) A method of providing a key container according to claim 1, wherein once the request has been received, the method further comprises the step of generating the requested key container.

25. (Previously presented) A method of providing a key container according to claim 1, wherein the request is made using a computer communication protocol selected from the group consisting of Lightweight Directory Access Protocol (LDAP), Directory Access Protocol (DAP), Certification Management Protocol (CMP), XML Key Management Specification (XKMS), and HyperText Transfer Protocol (HTTP).

26. (Previously presented) A method of providing a key container according to claim 1, wherein the key container contains a cryptographic key that is a public key.

27. (Previously presented) A method of providing a key container according to claim 1, wherein the key container is a digital certificate.

28. (Previously presented) A method of providing a key container according to claim 1, wherein the key container is a Pretty Good Privacy (PGP) public key.

29. (Previously presented) A method of providing a key container according to claim 1, wherein the address contained in the key container is an e-mail address and the gateway is an e-mail gateway.

30. (Previously presented) A method of providing a key container according to claim 1, wherein the key container is provided for a specific message.

31. (Previously presented) A method of providing a key container according to claim 1, wherein the key container contains information that invalidates its use at a time in the future.

32. (Original) A method of providing a key container according to claim 31, wherein the time is of sufficiently short duration that the key container can be used for only a few messages.

33. (Previously presented) A method of providing a key container according to claim 1, wherein the key container contains the same container identifiers of the key container of the gateway.

34. (Previously presented) A method of providing a key container according to claim 1, wherein the key container is an encryption key container to be used for encryption operations.

35. (Original) A method of providing a key container according to claim 34, wherein the key container contains a parameter that indicates that the key container is to be used for encryption functions.

36. (Previously presented) A method of providing a key container according to claim 1, wherein the key container secures the message through use of the cryptographic key to encrypt the message.

37. (Previously presented) A method of providing a key container according to claim 1, wherein the sender's address is from the same domain as the gateway.

38. (Previously presented) A method of providing a key container according to claim 1, wherein the key container is a signing key container.

39. (Previously presented) A method of providing a key container according to claim 1, wherein the key container contains a parameter that indicates that the key container is to be used for signing operations.

40. (Previously presented) A method of providing a key container according to claim 1, wherein the key container secures the message by being carried with the message.

41. (Previously presented) A method of providing a key container according to claim 1, wherein the key container includes information that permits a requestor to determine the authenticity and integrity of the key container.

42. (Previously presented) A method of providing a key container according to claim 1, wherein the key container contains security preferences of the gateway.

43. (Previously presented) A method of providing a key container according to claim 1, wherein the key container includes information about the key container directory that provided the key container.

44. (Previously presented) A key container directory operable to provide a key container according to the method of claim 1, wherein the key container directory is remote from the gateway.

45. (Original) A key container directory according to claim 44, wherein the key container has a datastore of cryptographic keys that can be contained in any provided key container.

46. (Original) A method of receiving a key container comprising the steps of:

sending a request to a key container directory for a key container to be used to secure a message that is transmitted from a sender to a recipient; and

receiving from the key container directory the key container that contains the cryptographic key of a gateway that the message will transit and an address of the sender or the recipient.

47. (Original) A method of receiving a key container according to claim 46, wherein the method is performed by the sender of the message.

48. (Previously presented) A method of receiving a key container according to claim 46, wherein the step of sending a request for the key container includes an indication that an encryption key container is requested.

49. (Previously presented) A method of receiving a key container according to claim 46, wherein the step of sending the request for the key container includes the address of the recipient.

50. (Previously presented) A method of receiving a key container according to claim 46, wherein the method further comprises the step of encrypting the message using the cryptographic key contained in the key container.

51. (Previously presented) A method of receiving a key container according to claim 46, wherein the key container is an encryption key container to be used for encryption operations.

52. (Previously presented) A method of receiving a key container according to claim 46, wherein the key container contains a parameter that indicates that the key container is to be used for encryption functions.

53. (Previously presented) A method of receiving a key container according to claim 46, wherein the key container secures the message through use of the cryptographic key to encrypt the message.

54. (Previously presented) A method of receiving a key container according to claim 46, wherein the sender's address is from the same domain as the gateway.

55. (Original) A method of receiving a key container according to claim 46, wherein the method is performed by the gateway.

56. (Previously presented) A method of receiving a key container according to claim 46, wherein the step of sending the request for the key container includes an indication that a signing key container is requested.

57. (Previously presented) A method of receiving a key container according to claim 46, wherein the step of sending the request for the key container includes the address of the sender.

58. (Currently amended) A method of receiving a key container according to ~~any one of claims~~ claim 46 ~~or 55 to 57~~, wherein the key container is a signing key container.

59. (Previously presented) A method of receiving a key container according to claim 46, wherein the key container contains a parameter that indicates that the key container is to be used for signing operations.

60. (Previously presented) A method of receiving a key container according to claim 46, wherein the key container secures the message by being carried with the message.

61. (Previously presented) A method of receiving a key container according to claim 46, wherein the key container includes information that permits a requestor to determine the authenticity and integrity of the key container.

62. (Previously presented) A method of receiving a key container according to claim 46, wherein the key container contains security preferences of the gateway.

63. (Previously presented) A method of receiving a key container according to claim 46, wherein the key container includes information about the key container directory that provided the key container.

64. (Previously presented) An e-mail client that is operable to perform the method of receiving a key container according to claim 46.

65. (Previously presented) A gateway that is operable to perform the method of receiving a key container according to claim 46.

66. (Original) A key container to be used to secure a message that is transmitted from a sender to a recipient using a gateway, wherein the key container contains a cryptographic key of the gateway, an address of the sender or the recipient and information that invalidates the use of the key container at a time in the future.

67. (Cancelled)

68. (Cancelled)

69. (Cancelled)